Information Management and Technology (IMT) Awareness

Glossary

A

Access to Privacy Act Records

Each agency that maintains a system of records shall, upon request by any individual to gain access to his/her record or to any information pertaining to him/her which is contained in the system, permit him/her and upon his/her request, a person of his/her own choosing to accompany him/her, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him/her, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

Accountability

Ethics: The readiness or preparedness to give an explanation or justification for one's judgments, intentions, acts and omissions when appropriately called upon to do so.

Technology: the traceability of actions performed on a system to a user, process or device. For example, the unique user identification and authentication supports accountability; the use of shared user IDs and passwords inhibits accountability.

Agency Records

"Records that are either created or obtained by an agency and are under agency possession and control at the time of a FOIA request, or is maintained by an entity under Government contract for the purposes of records management."

Assistive Technology (AT)

Assistive technology (AT) is a device or software used to increase, maintain or improve the functional capabilities of individuals with disabilities. It is sometimes referred to as adaptive technology. Examples of AT include voice input, screen readers (voice output), telecommunications devices for the deaf, alternative keyboards, screen magnification software and switch-based input.

Associate Privacy Officer

The Privacy Official within a bureau or office who administers the privacy functions of the bureau or office, under the general guidance of the Departmental Privacy Officer. This includes working with program offices to develop and revise system of records notices, conduct privacy impact assessments, fulfill privacy reporting requirements on behalf of the bureau or office, serve as a subject matter expert on privacy matters, and lead breach response and remediation activities for their bureau or office.

Attended Fax

An attended fax is a means by which an employee can safely transmit PII across distances. To carry out an attended fax, first ensure you have the correct fax number. Then telephone the recipient and make sure that person is standing by to receive the fax. Submit the fax, then double-check to ensure in the fax confirmation that it went to the correct number and that all pages were successfully sent.

B

Breach

A breach is the loss of control, compromise, unauthorized disclosure, or unauthorized acquisition, or any similar occurrences where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

Bureau

A bureau is any constituent component of the Department. The Office of the Secretary (which includes all of the Departmental offices as well as other offices), the Office of the Solicitor, and the Office of the Inspector General are also considered as bureaus.

Bureau/Office FOIA Officer

The person within a bureau or office who administers the Freedom of Information Act with that bureau or office, under the overall guidance of the Departmental FOIA Officer. This includes acknowledging and responding to FOIA requests to the bureau or office, determining the Action Office responsible for preparing the response, applying exemptions, and participating in FOIA reporting requirements on behalf of the bureau or office.

Bureau/Office Information Collection Clearance Officer

The person within a bureau or office who administers the Paperwork Reduction Act for that bureau or office, including working with program offices to develop the proper notices and Supporting Statement for new and existing information collections under the Paperwork Reduction Act.

C

Chief Information Officer (CIO)

The Department has an overall Chief Information Officer who also serves, at DOI, as the SAOP (Senior Agency Official for Privacy) for Records Management.

Civil Liberties

Fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights

Rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term civil rights involves positive (or affirmative) government action to protect against infringement, while the term civil liberties involves restrictions on government.

Code of Federal Regulations (CFR)

The Code of Federal Regulations is the codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

D

Departmental Manual (DM)

The written policy decisions of each cabinet level department.

Departmental Privacy Officer

The Departmental Privacy Officer (DPO) is the official within the OCIO designated to carry out the privacy functions delegated by the SAOP, and is responsible for managing an agency-wide privacy program for administrative, management and compliance activities to ensure compliance with Federal privacy laws, regulations and policies. This includes promulgation of privacy policies and procedures, oversight of bureau/office privacy programs, coordination of all privacy activities, and preparation of privacy reports to external entities with bureau or office assistance.

Departmental Records Schedule (DRS)

Department-wide records retention and disposition schedule composed of eight parts. Two are currently approved by the Archivist of the United States: Administrative and Policy Records Schedules.

DI-3710 Disclosure Accounting Form

Official DOI form used to record the date, nature and purpose of each disclosure from a Privacy Act systems of records, and the name and address of the individual or agency to whom the disclosure is made (See the Privacy Act, 5 U.S.C. 552a (c) for requirements to account for records disclosed to external parties).

Disclosure

Disclosure means release of information contained in a system of records to any person (other than the person to whom the information pertains), including any employee of the Department of the Interior and employees of other Federal departments and agencies.

Disposition

The actions taken regarding records no longer needed for current government business. For example, (1) transfer to agency storage facilities or Federal records centers, (2) transfer from one Federal agency to another, (3) transfer of permanent records to the National Archives and Administration, and (4) disposal of temporary records.

Dissemination

The government-initiated distribution of information to a nongovernment entity, including the public. The term 'dissemination,' as used within this Circular, does not include distribution limited to Federal Government employees, intra- or interagency use or sharing of Federal information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act (5 U.S.C. § 552a).

Documentary materials

A collection term for records, non-record materials, and personal papers that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording.

DOI-CIRC (DOI Computer Incident Response Center)

DOI's central reporting organization for computer incident response and tracking. All DOI incidents must be reported through the Associate Chief Information Security Officer to DOI-CIRC, who tracks these incidents and may report them to US-CERT. The DOI-CIRC coordinates threat identification and incident remediation with US-CERT. At DOI, it is an integral part of the Advanced Security Operations Center (ASOC).

DOI Privacy Act Regulations

The legal requirements derived by the elements addressed in the Privacy Act as applied to the Department of the Interior (43 CFR Part 2, Subpart K).

E

E-Government Act of 2002

The E-Government Act of 2002 was created to enhance the management and promotion of electronic government services and processes by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services. Section 208 institutes the requirement for Federal agencies to conduct Privacy Impact Assessments for all electronic systems or collections that contain PII on members of the public.

F

Fair Information Practice Principles (FIPPs)

Principles that are widely accepted in the United States and internationally as a general framework for privacy and that are reflected in various Federal and international laws and policies. In a number of organizations, the principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies.

Federal Information

Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal Information Security Modernization Act of 2014 (FISMA)

The Federal Information Security Modernization Act provides a comprehensive framework for ensuring the effectiveness of information security controls and addresses responsibilities of OMB, Department of Homeland Security, and Federal agencies. Agencies must ensure FISMA compliance and information security program requirements, such as policy, procedures, risk assessments, standards, training, remedial actions to address deficiencies, annual evaluations and procedures for reporting and responding to incidents. Agencies must also conduct reviews of their information security and privacy programs, and report the results to OMB to perform oversight responsibilities.

Federal Records

Federal records are documentary materials created or received in the transaction of government business, regardless of media.

Federal Records Act

The Federal Records Act of 1950, as amended, establishes the framework for records management programs in federal agencies.

Federal Records Center (FRC)

The FRCs provide a number of records management storage and retrieval services, including online management of records through the Archives and Records Centers Information System (ARCIS).

Federal Register

The *Federal Register* is the official government daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents. Privacy Act System of Records Notices, for example, are published in the *Federal Register*, as are notices associated with Paperwork Reduction Act compliance.

File Plan

A file plan lists all of the records created by a bureau or office Records Officer, or program staff, and maintained by an employee, contractor or staff member of that bureau or office. The office file plan should be applied to records in all media (e.g. paper, non-paper, and electronic).

File Station

File stations are designated areas in which to keep records that provide control and supervision over records; facilitate coordination between and among official file stations; and ensure uniformity in filing and retrieval of records.

Freedom of Information Act of 1966 (FOIA)

An Act designed to provide agency records upon request unless certain exemptions apply to all or part of the records. Refer to DOI FOIA regulations for more information about processing information under the FOIA that originated from the Privacy Act System of Records.

G

General Records Schedules (GRS)

Records schedules development by NARA that set a default retention for records common to most federal agencies. The GRS is considered mandatory unless superseded by an agency-specific records schedule (such as the DRS).

H

Hearing Disability

A hearing disability is a lack of or reduction in the ability to hear clearly. Hearing disabilities include:

- Deafness or complete inability to hear
- Being hard of hearing
- Inability to hear high- and/or low-frequency sounds

People with hearing disabilities may use captions, transcripts or amplification of audio content. They may rely on alternatives to voice input in order to use live voice mail or to participate in online chats.

High-Level Official

The term “High-Level Official” is used to refer to officials whose records are deemed to merit permanent retention based on the nature of the position itself. Officials are identified under this label because of their role in determining bureau/DOI policy and major decisions regarding the accomplishment of mission objectives. They may also be authorized to represent the bureau, DOI, or the Federal government to external national or international activities and parties.

Homeland Security Information

Any information possessed by a state, local, Tribal, or Federal agency that relates to a threat of terrorist activity or to the ability to prevent, interdict, or disrupt terrorist activity, or would improve the identification or investigation of a suspected terrorist or terrorist organization or the response to a terrorist act.

I

Identity Theft

Use of another’s personal information to commit fraud. Financial information, medical information, Social Security number, address, phone are all used. Crimes such as purchasing items under another person’s credit, and receiving medical services under another person’s insurance, transferring money from the owner’s financial accounts all constitute criminal acts. Occurrences of identity theft are dramatically increasing.

Impact

The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Incident

An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (44 U.S.C. § 3552).

Indian Fiduciary Trust records

Documents used in the management of Indian trust assets such as land, natural resources, and monies held in trust by the Federal government for individual Indians, Indian tribes, or Alaska natives and Alaska native organizations. The Department retains them permanently.

Individual

For purposes of the Privacy Act, an individual means a citizen of the United States or an alien lawfully admitted for permanent residence.

Information

A collection of related data; knowledge about a topic. Data that have been processed into a format that is understandable by its intended audience.

Information and Communication Technology (ICT)

Often used as an extended synonym for information technology (IT), but is a more specific term that stresses the role of unified communications and the integration of telecommunications, computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.

Information in Identifiable Form

Similar to PII, Information in Identifiable Form (or Identifiable Form) is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, Social Security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, (i.e., indirect identification). (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). See OMB Memorandum M-03-22.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: a) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; b) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and c) Availability, which means ensuring timely and reliable access to and use of information (44 U.S.C. § 3552).

Information Sharing Environment (ISE)

A framework that facilitates access to terrorism related information by all relevant entities through a combination of information sharing policies, procedures, and technologies.

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Life Cycle

All phases in the useful life of an information system, including planning, acquiring, operating, maintaining, and disposing.

Information Technology

Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use (40 U.S.C. § 11101).

Informational Value

The usefulness of records in documenting the persons, places, things, or matters dealt with by an agency, in contrast to documenting the agency's organization, functions, and activities. The value of information generally decreases with age.

Inspector General (IG) or Office of Inspector General (OIG)

An office created for federal agencies by the Inspector General Act of 1978. Sixty four federal IGs are appointed for life to investigate matters of corruption, waste, fraud (criminal), abuse (policy violation), mismanagement and inefficiency.

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

The Intelligence Reform and Terrorism Prevention Act of 2004 restructured the U.S. Government's intelligence community by coordinating and integrating activities among law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel in an effort to enhance the way we detect and respond to threats. The IRTPA also established the Information Sharing Environment to ensure access to and improve the coordination, integration, sharing, and use of terrorism and homeland security information between and among Federal, state, local, tribal, and territorial agencies, the private-sector, and foreign partners.

L

Litigation Hold

A legal notification from the Department or Office of the Solicitor directing employees to preserve any documentary materials that may be relevant to a pending or foreseeable lawsuit or administrative adjudication.

M

Maintain

The term *maintain* includes maintain, collect, use or disseminate activities. In fact, it can apply to any possible action, including storage, of information.

Medical Information

Medical information are records which relate to the identification, prevention, cure or alleviation of any disease, illness or injury including psychological disorders, alcoholism and drug addiction.

Motor Disability

Motor disabilities include a broad range of physical impairments, from minor conditions to profound disabilities that restrict voluntary movement. Conditions that may cause motor disabilities include:

- Repetitive Stress Injury (RSI)
- Arthritis
- Stroke
- Amyotrophic Lateral Sclerosis (ALS)
- Spinal Cord injury
- Loss of limbs or digits
- Short-term disability, such as a broken arm

People with motor disabilities may use the keyboard, an on-screen keyboard, voice recognition software or another alternative input device rather than a mouse for all interactions with software and web pages.

Multimedia

Software and applications that combine text, high-quality sound, two- and three-dimensional graphics, animation, photo images, and full-motion video.

N

National Archives and Records Administration

The National Archives and Records Administration (NARA), as an independent Federal agency, is America's national record keeper. Its mission is to ensure ready access to the essential evidence that documents the rights of American citizens, the actions of Federal officials, and the national experience, and the discovery, use, and knowledge from this documentary heritage.

National Institute of Standards and Technology (**NIST**)

NIST sets standards for many types of technical performance, including information technology systems and their security. Federal agencies are required to adhere to NIST standards regarding numerous aspects of security for information technology.

Need to know

According to the Privacy Act, it pertains to those officers and employees of an agency which maintains the record who have a need for the record in the performance of their duties. (Applies to intra-agency.) Also, a basic Information Assurance principle supporting confidentiality.

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Non-Records

Non-records are materials used solely for reference, exhibition or convenience purposes. An individual's personal papers are not Federal records even if kept in the office or work area.

O

Office of Management and Budget

The Office of Management and Budget's (OMB's) predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise its administration in Executive Branch agencies. OMB has oversight over government Privacy Act implementation and the development of Federal regulations. OMB also oversees Federal implementation of the Paperwork Reduction Act.

Organization

An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

P

Paperwork Reduction Act of 1995

The Paperwork Reduction Act of 1995 requires agencies to plan for the development of new collections of information and the extension of ongoing collections well in advance of sending proposals to OMB. Agencies must: seek public comment on proposed collections of information through "60-day notices" in the *Federal Register*; certify to OMB that efforts have been made to reduce the burden of the collection on small businesses, local government, and other small entities; and have in place a process for independent review of information collection requests prior to submission to OMB. Each bureau or office has an Information Collection Clearance Officer which carries out these duties on behalf of the bureau or office.

Personal Information

Equates to PII or Privacy Information; see below.

Personal papers

Personal papers are documentary materials, or any reasonably segregable portion thereof, of a private or nonpublic character that do not relate to or have any effect upon the conduct of agency business.

Personally Identifiable Information (PII)

Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. For example, such information may include a name, username, SSN, date and place of birth, phone number, home address, email address, credit card number, account number, driver's license number, vehicle license number, photograph, biometric identifier (e.g., facial recognition, fingerprint), educational information, financial information, medical information, criminal or employment information, or any information created specifically to identify or authenticate an individual (e.g., a random generated number).

Portable Storage Device

An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Privacy

The right to be left alone and the right to control conditions under which information pertaining to individuals is collected, disseminated and used. The International Association of Privacy Professionals defines Privacy as "The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual's expectations; also, the right of an individual to control the collection, use, and disclosure of personal information."

Privacy Act of 1974

The Privacy Act (5 U.S.C. 552a) established controls over what personal information the Federal Government collects and how it uses or discloses that information. The Privacy Act has four basic objectives: (1) To restrict disclosure of personally identifiable records maintained by agencies; (2) To grant individuals increased rights of access to agency records maintained on them; (3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete; and (4) To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Privacy Act Statement

A disclosure statement provided to an individual when PII is directly collected for a Privacy Act system of records. The Privacy Act Statement provides the legal authority and purpose for the collection, the routine uses of the information, and who will have access to the information, and discloses whether providing the information is voluntary or mandatory, and any consequences for not providing the information. The Privacy Act Statement may be provided on a form, in a separate handout, read to the individual, or prominently posted.

Privacy Control

The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

Privacy Impact Assessment (PIA)

An analysis and a formal document detailing the process and the outcome of the analysis that is required whenever an information technology system, technology, program, project, information collection, or other activity involves the use of PII, has privacy implications, or otherwise impacts individual privacy as determined by the Senior Agency Official for Privacy. A PIA is a tool that analyzes privacy risk and describes what information DOI is collecting, why the information is being collected, how the information is used, stored, and shared, how the information may be accessed, how the information is protected from unauthorized use or disclosure, and how long information is retained.

Privacy Information

PII or personal information includes any information linked, or linkable, to a named individual, whether directly named or indirectly inferred. Such information includes the individual's full name, SSN, home address, home telephone number, finger and voice prints, birth date, medical, financial and family information, beliefs and affiliations, and any other information that is identifiable to the individual

Privacy Notice

A notice that informs individuals of activities that may have privacy implications, and discloses some or all the ways PII may be gathered, used, managed and disclosed. A Privacy Notice is provided when PII is present or collected but may not necessarily be maintained in a Privacy Act system. The Privacy Notice has the same requirements as a Privacy Act Statement and must include the authority and purpose for collecting information, the uses of information, any sharing or dissemination of information, and the consequences of not providing information. A Privacy Notice may also be called a Privacy Act Statement.

Privacy Policy

A single, centrally located statement that is accessible from an agency's official homepage. The Privacy Policy is a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities.

R

Record

All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them (44 U.S.C. § 3301).

A record according to the Privacy Act is any item, collection, or grouping of information about an individual that is maintained by an agency.

Records Inventory

Creating a Records Inventory is the first step in establishing a records management program. An office's records inventory identifies categories of records, the disposition authorities applicable to them, volume of records, and their location in the office (whether physical or electronic). Records inventories are used to support the transfer, archival, and destruction of Federal records, and are a critical supporting element of an office's File Plan. Inventories are expected to be updated as the records holdings of the office change.

Records Officer

The Department of the Interior Records Officer is responsible for providing leadership and direction for the Department's records management program. The program properly identifies recordkeeping requirements and manages needed records throughout their life cycle.

Records Retention and Disposition Schedules, *or Records Schedules*

Schedules that identify various categories of records, and establish the retention period and ultimate disposition for each category. Disposition of the records are either temporary or permanent.

Redress

The complaint resolution process for handling privacy inquiries and complaints as well as for allowing citizens who believe that agencies are storing and using erroneous information about them to gain access to and correct that information.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Management

The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Routine Use

A use of a record for a purpose which is compatible with the purpose for which it was collected (these are identified in the Privacy Act system of records notice published in the *Federal Register*). It is important the agency employees comply with the limits of the routine uses.

S

Safeguards

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Security

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Control

The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Senior Agency Official for Privacy (SAOP)

OMB requires that each agency designate an SAOP for that agency. At the Department of the Interior, the Chief Information Officer is designated as the SAOP. The SAOP is the official with overall responsibility and accountability for implementing and managing an agency-wide privacy program, and overseeing governance, data protection, and compliance activities in alignment with Federal privacy laws, regulations, and policies.

Sensitive PII

PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some types of PII, such as SSNs, credit card numbers, and biometric identifiers, are always sensitive and must be safeguarded against unauthorized disclosure. Some types of PII may become sensitive PII when maintained or combined with other types of PII or identifying information about the individual. The context surrounding the use of PII is also important to determine whether it is sensitive PII. For example, a list of employee names by itself may not be considered sensitive PII, but a list of employees who received poor performance ratings is sensitive PII.

Screen Magnification

Screen magnification software enlarges the text on screen and can provide users with options to adjust color contrast. Examples of screen magnification software are ZoomText and Magic.

Screen Reader

A screen reader is text-to-speech software that interprets the content of a screen and relays the information to the user. This software "reads" what is displayed on the screen, including email, documents and spreadsheets. Examples of screen reader software are JAWS and Window-Eyes.

Section 508

Section 508 of the Rehabilitation Act requires that Electronic and Information Technology (EIT) developed, procured, maintained or used by the Federal government be accessible to persons with disabilities. To provide maximum accessibility to all users, the Section 508 guidelines specify functional performance criteria that essentially define the spirit of the law. These criteria require that all EIT products and services be fully operational to all users, including those with vision, hearing, speech or motor control impairments, or that they be designed to work compatibly with the assistive technology used by persons with disabilities.

Speech Recognition Software

Speech recognition software allows users, primarily those with mobility impairments, to input text and control the computer by voice. An example of speech recognition software is Dragon NaturallySpeaking.

System

A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization.

System of Records

A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual (also referred to as a “Privacy Act System”).

System of Records Notice (SORN)

The statement providing the public notice of the existence and character of a group of any records under the control of any agency in which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires that this notice be published in the *Federal Register* upon establishment or substantive revision of a system of records, and establishes what information about the system must be included.

T

Telework

A term referring to substituting telecommunications for any form of work-related travel.

Third-party websites or applications - The term “third-party websites or applications” refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a “.com” website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official website.

Transitory Federal Records

Records that contain information directly related to the Department’s mission, operations, and activities, but they are of short term interest (under 180 days) and have minimal or no documentary or evidentiary value.

U

United States Code (USC)

The United States Code is the codification by subject matter of the general and permanent laws of the United States. It is divided by broad subjects into 50 titles and published by the Office of the Law Revision Counsel of the U.S. House of Representatives.

V

Visual Disability

A visual disability is a lack of or reduction in the ability to see. Visual disabilities include:

- Total blindness
- Visual impairment: having restricted central and/or peripheral vision
- Color blindness: inability to see or recognize certain colors or combinations of colors

People with visual disabilities may use screen magnification software or screen readers. They may rely on information conveyed by a means other than color. Screen reader users may interact with software and web pages using a keyboard rather than a mouse.

W

Written consent

Written consent is provided by the subject of the file to release information from the subject's file.